UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/533,120	09/19/2005	Bernard Smeets	2380-889	7035

23117 7590 06/03/2010

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
06/03/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/533,120	SMEETS ET AL.	
	Examiner	Art Unit	
	MICHAEL PYZOCHA	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 April 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-50,52 and 54-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47-50,52 and 54-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/19/09, 5/19/10*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

1. Amendment filed 04/01/2010 has been received and considered.

2. Claims 47-50, 52 and 54-75 are pending.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 11/19/2009 and 05/19/2010 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 47-50, 52 and 54-75 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Applicant has cited various lines on pages 15 and 19 for support for the newly claimed limitation: "unknown after being stored in the storage device or option"; while this portion provides support for keeping the secret unknown from unauthorized parties

after being stored on the storage device, the specification makes no mention of any "option". As such these claims contain information not supported by the specification.

Applicant has cited various lines on pages 22 and 24 for support for the newly claimed limitation: "not stored in a memory such that the temporarily available instance of the device-specific security data is only available as long as the extemally received trigger data is received"; these portions relate to generating, in response to trigger data, the security data. There is no mention of performing these steps without memory or as long as the trigger data is provided, as claimed. The mere absence of a positive recitation in the specification is not basis for an exclusion by way of negative limitations (see MPEP 2173.05(i)).

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 47-50, 52 and 54-75 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claims 47, 66 and 70 recite the limitation, "unknown after being stored in the storage device or option". It is unclear to what the "option" refers and it is further unclear how data can be stored in an option. As such this limitation renders the claim indefinite.

9. Any claims not specifically addressed are rejected by virtue of their dependencies.

Specification

10. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: the specification is objected to for similar reasons as put forth above with respect to the rejections under 35 USC 112 1st.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 47, 48, 52, 54, 58-61, 66, 67, 69-71, 73 and 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (US 20020099948) in view of Richards (US 20010054147), in view of Knapen (US 20030053629) and further in view of Fruehauf et al. (US 7149308).

As per claims 47, 66 and 70, Kocher et al. discloses a tamper-resistant electronic circuit for implementation in a device, said tamper-resistant electronic circuit comprising: a storage device for tamper-resistantly storing, during manufacture of the tamper-resistant electronic circuit, a random secret not accessible over any external circuit interface to the tamper-resistant electronic circuit and unknown after being stored in the storage device or option (see paragraphs [0078], [0081], [0104] and claim 1 where it is unknown to unauthorized entities); trigger data generating circuitry for, during

configuration of the tamper-resistant electronic circuit, generating trigger data using the random secret and device-specific security data that is different from the random secret; a receiver for, during operation of the configured tamper-resistant electronic circuit by a user, receiving external to the tamper-resistant electronic circuit from the user via an external circuit interface the trigger data (see paragraph [0078] and claim 1 steps (a)-(c) where the group verification result is the trigger data); a cryptographic processing engine, in response to the externally received trigger data from the user, for performing cryptographic processing at least partly in response to said stored secret and the externally received trigger data from the user to generate an instance of the device-specific security data internally confined within said electronic circuit during usage of said device; and electronic circuitry, connected to the cryptographic processing engine and configured to perform a security-related operation in response to said internally-confined, device-specific security data (see paragraph [0078] and claims 1 step (c)).

Kocher et al. fails to explicitly disclose outputting the trigger data and that the security data is temporary.

However, Richards teaches outputting triggering data (see paragraph [0035]) and Knapen teaches generating temporary keys based on received triggering data (see Abstract and paragraphs [0017] and [0021]-[0023]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to output the trigging data and to create temporary security data in the Kocher et al. system.

Motivation to do so would have been to authorize the enablement of an action (see Richards paragraph [0035]) and as recognized by one of ordinary skill in the art to use temporary keys to limit the ability of attackers to break the encryption.

The modified Kocher et al., Richards and Knapen system fails to disclose that the security data is not stored in a memory such that the temporarily available instance of the device-specific security data is only available as long as the externally received trigger data is received.

However, Fruehauf et al. teaches a system where security data is only temporarily available (i.e. not stored in memory) when trigger data is received (see column 7 line 57 through column 8 line 22 where the seed is the trigger data the temporary keys are generated using the temporary seed until this seed is replaced by the permanent seed).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to temporarily use security data in the modified Kocher et al., Richards and Knapen system.

Motivation to do so would have been to allow for configuration of the device (see Fruehauf et al. column 7 line 57 through column 8 line 22).

As per claims 48, 67 and 71, the modified Kocher et al., Richards, Knapen and Fruehauf et al. system discloses said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication (see Kocher et al. Abstract).

As per claims 52, 54, 69, 73 and 75, the modified Kocher et al., Richards, Knapen and Fruehauf et al. system discloses creating and using triggering data based from cryptographic functions (see Kocher et al. paragraph [0078] and Richards paragraph [0035]).

As per claims 58-61, the modified Kocher et al., Richards, Knapen and Fruehauf et al. system discloses performing additional cryptographic processing based on the internally-confined device-specific security data and external data to generate further security data and performing security-related operations in response to said security data where the system is configured to generate and use certain encryption keys (see Kocher et al. Abstract and paragraphs [0051], [0062]).

13. Claims 49, 50, 68 and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Kocher et al., Richards, Knapen and Fruehauf et al. system as applied to claims 47, 66 and 70 above, and further in view of Venkatesan et al. (US 20040001605).

As per claims 49, 50, 68 and 72, the modified Kocher et al., Richards, Knapen and Fruehauf et al. system fails to explicitly disclose that the device is configured for producing digital content by marking (by embedding a fingerprint in) said digital content based on the internally-confined temporal device-specific security data.

However, Venkatesan et al. teaches marking produced content with specific security information (see paragraph [0053]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the device specific security information of the modified Kocher et al., Richards, Knapen and Fruehauf et al. system to watermark produced content.

Motivation to do so would have been to uniquely identify the content as original (see Venkatesan et al. paragraph [0053]).

14. Claims 55-57 and 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Kocher et al., Richards, Knapen and Fruehauf et al. system as applied to claims 47 and 73 above, and further in view of Beatson (US 20030056100).

As per claims 55-57 and 74, the modified Kocher et al., Richards, Knapen and Fruehauf et al. system disclose authenticating a manufacturer and providing information to the manufacturer (see Kocher et al. paragraphs [0081] and [0104]), but fails to disclose allowing/preventing access to the security information based on an access code.

However, Beatson teaches and access code to prevent/allow access to a device (see Beatson paragraph [0084]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to require an access code to use the device of the modified Kocher et al., Richards, Knapen and Fruehauf et al. system.

Motivation, as recognized by one of ordinary skill in the art, to do so would have been to prevent unauthorized access to the security data.

15. Claims 62-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Kocher et al., Richards, Knapen and Fruehauf et al. system as applied to claim 47 above, and further in view of Hopkins et al. (EP 1081891).

As per claims 62-64, the modified Kocher et al., Richards, Knapen and Fruehauf et al. system fails to explicitly disclose generating an internally-confined private key based at least partially on said stored secret and using the private key and corresponding public key to generate a shared key.

However, Hopkins et al. teaches such key generation/exchange (see paragraphs [0039] and [0046] through [0053]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to generate and exchange keys in the modified Kocher et al., Richards, Knapen and Fruehauf et al. system.

Motivation to do so would have been to set-up a secure communications session (see Hopkins et al. paragraphs [0039] and [0046] through [0053]).

16. Claim 65 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Kocher et al., Richards, Knapen and Fruehauf et al. system as applied to claim 47 above, in view of Xiao et al. (WO 0077974) and further in view of Matyas, Jr. et al. (US 6687375).

As per claim 65, the modified Kocher et al., Richards, Knapen and Fruehauf et al. system fails to disclose generating a chain of keys by hashing a previous key with an identity.

However, Xiao et al. teaches chaining based off values of keys (see page 9 lines 1-10) and Matyas, Jr. et al. teaches creating a key by hashing a key with identity information (see FIG. 4 and column 9 lines 3-17).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to create a chain of user dependent keys in the modified Kocher et al., Richards, Knapen and Fruehauf et al. system.

Motivation to do so would have been to create a chain of trust (see Xiao et al. page 9) and to create a user specific key (see Matyas, Jr. et al. column 9 lines 3-17).

Response to Arguments

17. Applicant's arguments with respect to claims 47-50, 52 and 54-75 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Primary Examiner, Art Unit 2437